UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA

BELINDA ARNOLD, individually and on behalf of all others similarly situated, Plaintiff, v. CNO FINANCIAL GROUP, INC. and BANKERS LIFE AND CASUALTY COMPANY, Defendants.	Case No. 1:24-cv-00334 JRS-MJD JURY DEMAND

AMENDED CLASS ACTION COMPLAINT

Plaintiff Belinda Arnold ("Plaintiff") brings this amended class action against Defendants CNO Financial Group, Inc. and Banker's Life and Casualty Company ("Defendants") for their failure to properly secure and safeguard Plaintiff's and Class Members' personally identifiable information ("PII") stored within Defendants' information network.

INTRODUCTION

1. Defendants comprise insurance and financial services company based in Indiana; Bankers Life and Casualty Company is a subsidiary of CNO Financial Group, Inc.[1]

2. Defendants acquired, collected, and stored Plaintiff's and Class Members' PII.

3. At all relevant times, Defendants knew or should have known, that Plaintiff and Class Members would use Defendants' services to store and/or share sensitive data, including

[1] https://www.bankerslife.com/about-us/bankers-life-history/ (last accessed February 21, 2024).

highly confidential PII.

4. On no later than November 29, 2023, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII as hosted with Defendants, with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

5. The total number of individuals who have had their data exposed due to Defendants' failure to implement appropriate security safeguards is approximately 45,842 people.[2]

6. Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, and is generally defined to include certain identifiers that do not on their face name an individual, but that is considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

7. The vulnerable and potentially exposed data at issue of Plaintiff and the Class stored on Defendants' information network includes, without limitation: names, Social Security numbers, dates of birth, and policy numbers.

8. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/1c0e29fa-a97f-4b3e-bd73-4f20e205b77f.shtml (last accessed February 21, 2024).

9. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

10. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

11. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendants.

12. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

13. Defendants are headquartered and routinely conducts business in the State where this district is located, has sufficient minimum contacts in this State, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State.

14. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Defendants do business in this Judicial District.

THE PARTIES

Plaintiff Belinda Arnold

15. Plaintiff Belinda Arnold is an adult individual and, at all relevant times herein, a resident and citizen of California, residing in Colusa, California. Plaintiff is a victim of the Data Breach.

16. Plaintiff's information was stored with Defendants as a result of their dealings with Defendants.

17. As required in order to obtain services from Defendants, Plaintiff provided Defendants with highly sensitive personal information who then possessed and controlled it.

18. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

19. At all times herein relevant, Plaintiff is and was a member of the Class.

20. Plaintiff received a letter from Defendants, dated January 26, 2024, stating that their PII was involved in the Data Breach (the "Notice").

21. Plaintiff was unaware of the Data Breach until receiving that letter.

22. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

23. Plaintiff was also injured by the material risk to future harm they suffer based on Defendants' breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including Social Security numbers, is highly

sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendants' clientele, that some of the Class's information that has been exposed has already been misused.

24. Plaintiff suffered actual injury in the form of damages to and diminution in the value of their PII—a condition of intangible property that they entrusted to Defendants, which was compromised in and as a result of the Data Breach.

25. Plaintiff, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PII.

26. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

27. Plaintiff has a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Defendant CNO Financial Group, Inc

28. Defendant CNO Financial Group, Inc. ("CNO") is a Delaware corporation. CNO was formed and organized under the laws of Delaware. CNO is headquartered in Carmel, Indiana with its principal office located at 11825 N. Pennsylvania Street, Carmel, Indiana 46032. CNO is therefore a citizen of the State of Indiana and State of Delaware for purposes of diversity jurisdiction under 28 U.S.C. § 1332.

Defendant Bankers Life and Casualty Company

29. Defendant Bankers Life and Casualty Company ("Bankers Life") is an Illinois

corporation with its principal place of business located in Chicago, Illinois, in Cook County at 303 E. Wacker Drive., Suite 500, Chicago, Illinois. Bankers Life has tens of thousands of customers located throughout the United States.

30. Bankers Life is a subsidiary of CNO.

CLASS ACTION ALLEGATIONS

31. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themself and the following Class:

> All individuals within the United States of America whose PII was exposed to unauthorized third-parties as a result of the data breach experienced by Defendants on November 29, 2023.

32. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

33. Plaintiff reserves the right to amend the above definitions or to propose subclasses in subsequent pleadings and motions for class certification.

34. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

35. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class are so numerous that

joinder of all members is impractical, if not impossible.

36. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendants had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII;

b. Whether Defendants knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. How and when Defendants actually learned of the Data Breach;

h. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the

loss of the PII of Plaintiff and Class Members;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendants' wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

37. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein.

38. Adequacy of Representation: Plaintiff in this class action is an adequate representative of the Class in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature.

39. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the class in its entirety. Plaintiff anticipates no management difficulties in this litigation.

40. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of

individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

41. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

42. This class action is also appropriate for certification because Defendants has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

43. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendants' conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

44. Unless a Class-wide injunction is issued, Defendants may continue failing to properly secure the PII of Class Members, and Defendants may continue to act unlawfully as set forth in this Complaint.

45. Further, Defendants has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to

the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

COMMON FACTUAL ALLEGATIONS

Defendants' Failed Response to the Breach

46. Not until after months it claims to have discovered the Data Breach did Defendants begin sending the Notice to persons whose PII Defendants confirmed was potentially compromised as a result of the Data Breach.

47. The Notice included, *inter alia*, basic details of the Data Breach, Defendants' recommended next steps, and Defendants' claims that it had learned of the Data Breach on November 29, 2023, and completed a review thereafter.

48. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

49. Defendants had and continues to have obligations created by applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

50. Plaintiff and Class Members were required to provide their PII to Defendants as a result of their dealings, and in furtherance of this relationship, Defendants created, collected, and stored Plaintiff and Class Members with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

51. Despite this, Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PII going forward.

52. Plaintiff and Class Members are, thus, left to speculate as to where their PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendants intend to enhance their information security systems and monitoring capabilities to prevent further breaches.

53. Unauthorized individuals can now easily access the PII of Plaintiff and Class Members.

Defendants Collected/Stored Class Members' PII

54. Defendants acquired, collected, and stored and assured reasonable security over Plaintiff's and Class Members' PII.

55. As a condition of its relationships with Plaintiff and Class Members, Defendants required that Plaintiff and Class Members entrust Defendants with highly sensitive and confidential PII.

56. Defendants, in turn, stored that information in the part of Defendants' system that was ultimately affected by the Data Breach.

57. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

58. Plaintiff and Class Members have taken reasonable steps to maintain the

confidentiality of their PII.

59. Plaintiff and Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

60. Defendants could have prevented the Data Breach, which began no later than November 29, 2023, by adequately securing and encrypting and/or more securely encrypting their servers generally, as well as Plaintiff's and Class Members' PII.

61. Defendants' negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

62. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

Defendants Had an Obligation to Protect the Stolen Information

63. Defendants' failure to adequately secure Plaintiff's and Class Members' sensitive data breaches duties they owe Plaintiff and Class Members under statutory and common law.

64. Defendants were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[3]

[3] The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

65. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

66. Defendants owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

67. Defendants owed a duty to Plaintiff and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that the PII was adequately secured and protected.

68. Defendants owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in their possession, including not sharing information with other entities who maintained sub-standard data security systems.

69. Defendants owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in their data security systems in a timely manner.

70. Defendants owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

71. Defendants owed a duty to Plaintiff and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this

PII to Defendants.

72. Defendants owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

73. Defendants owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

74. PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

75. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[4]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[5]; and other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[6]

76. Identity thieves can use PII, such as that of Plaintiff and Class Members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration

[4] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed February 21, 2024).
[5] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed February 21, 2024).
[6] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed February 21, 2024).

fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

77. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

78. Here, Defendants knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

79. As detailed above, Defendants are sophisticated organizations with the resources to deploy robust cybersecurity protocols. They knew, or should have known, that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Plaintiff and Class Members. Therefore, their failure to do so is intentional, willful, reckless and/or grossly negligent.

80. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable

[7] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed February 21, 2024).

measures to ensure that their network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of the Class)

81. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

82. At all times herein relevant, Defendants owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks.

83. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession;

b. to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely

act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

84. Defendants knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

85. Defendants knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of their data security systems, and the importance of adequate security.

86. Defendants knew about numerous, well-publicized data breaches.

87. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

88. Only Defendants was in the position to ensure that their systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to them.

89. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII.

90. Because Defendants knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the PII contained therein.

91. Plaintiff's and Class Members' willingness to entrust Defendants with their PII

was predicated on the understanding that Defendants would take adequate security precautions.

92. Moreover, only Defendants had the ability to protect its systems and the PII is stored on them from attack. Thus, Defendants had a special relationship with Plaintiff and Class Members.

93. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendants, Plaintiff, and/or the remaining Class Members.

94. Defendants breached their general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third

party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train their employees not to store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

95. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

96. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

97. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PII to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII.

98. Defendants breached their duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

99. To date, Defendants have not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach their disclosure obligations to Plaintiff and Class Members.

100. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

101. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

102. Plaintiff's and Class Members' PII was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

103. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

104. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

105. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of

productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PII, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

106. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

107. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of the Class)

108. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

109. Through their course of conduct, Defendants, Plaintiff and Class Members

entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

110. Defendants required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining Defendants' services.

111. Defendants solicited and invited Plaintiff and Class Members to provide their PII as part of Defendants' regular business practices.

112. Plaintiff and Class Members accepted Defendants' offers and provided their PII to Defendants.

113. As a condition of their relationship with Defendants, Plaintiff and Class Members provided and entrusted their PII to Defendants.

114. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

115. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendants, in exchange for, amongst other things, the protection of their PII.

116. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

117. Defendants breached their implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

118. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Class)

119. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

120. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

121. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendants.

122. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

123. Defendants acted in bad faith and/or with malicious motive in denying

Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of the Class)

124. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

125. By their wrongful acts and omissions described herein, Defendants have obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

126. Defendants, prior to and at the time Plaintiff and Class Members entrusted their PII to Defendants, caused Plaintiff and Class Members to reasonably believe that Defendants would keep such PII secure.

127. Defendants was aware, or should have been aware, that reasonable patients and consumers would have wanted their PII kept secure and would not have contracted with Defendants, directly or indirectly, had they known that Defendants' information systems were sub-standard for that purpose.

128. Defendants was also aware that, if the substandard condition of and vulnerabilities in their information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

129. Defendants failed to disclose facts pertaining to their substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

130. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Plaintiff and Class Members the ability to make a rational and informed purchasing and servicing decision and took undue advantage of

Plaintiff and Class Members.

131. Defendants were unjustly enriched at the expense of Plaintiff and Class Members, as Defendants received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and or services (or provided those services) that did not satisfy the purposes for which they bought/sought them.

132. Since Defendants' profits, benefits, and other compensation were obtained improperly, Defendants is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

133. Plaintiff and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendants from their wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

COUNT V
BAILMENT
(On Behalf of Plaintiff and the Class)

134. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

135. Plaintiff, the Class Members, and Defendants contemplated a mutual benefit bailment when the Plaintiff and putative members of the Class transmitted their PII to Defendants solely for the purpose of obtaining insurance benefits.

136. Plaintiff and the Class entrusted their PII to Defendants for a specific purpose—to obtain insurance benefits—with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was

accomplished.

137. Defendants accepted the Plaintiff's and the Class's PII for the specific purposes of the provision of insurance benefits.

138. Defendants were duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiff's and the Class's PII.

139. Plaintiff's and the Class's PII was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than Plaintiff and the Class intended.

140. As set forth in the preceding paragraphs, Plaintiff and the Class Members were damaged thereby.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themself and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendants, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and

Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendants to delete and purge the PII of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendants' systems periodically;

f. prohibiting Defendants from maintaining Plaintiff's and Class

Members' PII on a cloud-based database;

g. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

h. requiring Defendants to conduct regular database scanning and securing checks;

i. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

j. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

k. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to monitor Defendants' networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendants to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal

identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Dated: March 25, 2024

Respectfully submitted,

By: */s/ Lynn A. Toops*

Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
T: (317) 636-6481
F: (317) 636-2593
ltoops@cohenandmalad.com

LAUKAITIS LAW LLC
Kevin Laukaitis*
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

**Pro Hac Vice admission forthcoming*

Attorneys for Plaintiff and the Class